Serial No. 09/741,411

A. Partyka 20

Claim Amendments

No claim is amended in this Amendment.

1   **1.** (previously presented) A method of authentication in a telemetry system, said method
2 comprising:

3   transmitting, by each of a plurality of transmitters, transmissions intermittently at time intervals
4 and at a plurality of frequencies independently of any receiver of said transmissions and independently of
5 any other of said plurality of transmitters, and

6   holding, by a receiver, simultaneously for each of said plurality of transmitters, data indicative of
7 an expected frequency and an expected time of at least one future transmission, and

8   authenticating transmissions based on an expected and actual transmission frequency and time.

1   **2.** (previously presented) The method of claim 1 wherein said expected transmission frequency
2 comprises estimate for transmitter reference frequency drift.

3   **3.** (previously presented) The method of claim 1 wherein said expected transmission time
4 comprises estimate for transmitter time reference drift.

1   **4.** (previously presented) The method of claim 1 wherein each of said plurality of transmitters
2 controls transmission frequency and time between transmissions based on frequency-time pattern that is
3 different for each of said plurality of transmitters.

1   **5.** (previously presented) The method of claim 1 wherein, each of said plurality of transmitters is
2 for varying encryption key between transmissions.

1   **6.** (previously presented) The method of claim 5 wherein said encryption key is varied based on
2 frequency-time pattern for controlling transmission frequency and time between transmissions.

1   **7.** (previously presented) The method of claim 1 wherein each of said plurality of transmitters is
2 for verifiable and variable modification of transmitted messages content based on frequency-time pattern
3 for controlling transmission frequency and time between transmissions.

1   **8.** (previously presented) A receiver for authenticating telemetry transmissions, said receiver
2 comprising:

3   logic for holding, simultaneously for each plurality of transmissions, data indicative of an
4 expected time and an expected frequency of at least one future transmission, wherein each said plurality

Serial No. 09/741,411

A. Partyka 20

5 of transmissions is transmitted by a different one of a plurality of transmitters, wherein each of said

6 plurality of transmitters is for transmitting transmissions intermittently at time intervals and at a plurality

7 of frequencies independently of any equipment that is capable of receiving any of said transmissions from

8 any of said plurality of transmitters, and

9   circuitry for receiving said transmissions;

10   wherein said receiver is for authenticating transmissions based on an expected and actual

11 transmission frequency and time.

1   9. (previously presented) The receiver of claim 8 wherein said expected transmission frequency

2 comprises estimate for transmitter reference frequency drift.

1   10. (previously presented) The receiver of claim 8 wherein said expected transmission time

2 comprises estimate for transmitter time reference drift.

1   11. (previously presented) The receiver of claim 8 wherein frequency and time of transmissions is

2 controlled according to a frequency-time pattern that is different for each of said plurality of transmitters.

1   12. (previously presented) The receiver of claim 8 wherein said receiver is for changing

2 decryption key between transmissions based on a frequency-time pattern for controlling frequency and

3 time of transmissions.

1   13. (previously presented) The receiver of claim 8 wherein said receiver, in operation,

2 authenticates transmissions based on verifiable and variable modification of transmission content.

1   14. (previously presented) The receiver of claim 13 wherein said verifiable modification is based

2 on frequency-time pattern for controlling transmission frequency and time.

1   15. (previously presented) A frequency hopping telemetry transmitter comprising:

2   circuit for transmitting transmissions intermittently, at time intervals and at various frequencies,

3 independently of any receiver of said transmissions, and

4   logic for providing a predetermined frequency-time pattern for controlling transmission frequency

5 and time between transmissions, and

6   wherein said transmitter is for varying encryption, for said transmissions, based, at least in part,

7 on said frequency-time pattern.

- 3 of 12 -

Serial No. 09/741,411   A. Partyka 20

1   16. (previously presented) The transmitter of claim 15 wherein said frequency-time pattern is

2   individually selected for said transmitter from a plurality of predetermined patterns.

1   17. (previously presented) The transmitter of claim 15 wherein said frequency-time pattern is

2   predetermined based on a transmitter identification.

1   18. (previously presented) A frequency hopping telemetry transmitter comprising:

2   circuit for transmitting transmissions intermittently, at time intervals and at various frequencies,

3   independently of any receiver of said transmissions, and

4   logic for providing a predetermined frequency-time pattern for controlling transmission frequency

5   and time between transmissions, and

6   wherein said transmitter is for modification of at least a portion of known data for transmission

7   using a modifier that is varied based, at least in part, on said frequency-time pattern.

1   19. (previously presented) The transmitter of claim 18 wherein frequency-time pattern is

2   individually selected for said transmitter from a plurality of predetermined patterns.

1   20. (previously presented) The transmitter of claim 18 wherein said frequency-time pattern is

2   predetermined based on a transmitter identification.

BEST AVAILABLE COPY